Offensive Security macOS Researcher Exam Report

OSMR Exam Report

student@youremailaddress.com, OSID: XXXX

2022-11-08

Contents

1 Offensive-Security OSMR Exam Documentation

The Offensive Security OSMR exam documentation contains all efforts that were conducted in order to pass the Offensive Security macOS Researcher exam. This report will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has the technical knowledge required to pass the qualifications for the Offensive Security macOS Researcher certification.

1.1 Objective

The objective of this exam is to solve four given assignments as described in the control panel. The student is tasked with following a methodical approach in analyzing and solving the assignments. The exam report is meant to be a writeup of the steps taken to solve the assignment, including any analysis performed and code written.

An example page has already been created for you at the latter portions of this document that should give you sample information on what is expected to pass this exam. Use the sample report as a guideline to get you through the reporting, while removing any headlines that are not relevant to a specific assignment.

1.2 Requirements

The student will be required to fill out this exam documentation fully and to include the following sections:

- High-Level summary of assignment solutions.
- Methodology walkthrough and detailed outline of steps taken through analysis and all written code.
- Each finding with included screenshots, walkthrough, sample code or reference.
- Screenshots of proofs.

2 High-Level Summary

A brief description of the assignments that were solved, including the overall exploitation steps.

2.1 Assignment X

2.2 proof.txt / local.txt / secret.txt

Provide the contents of local.txt, proof.txt or secret.txt.

2.3 Initial Analysis

Provide relevant techniques and methods used to perform enumeration and discovery of the application and/or the environment. The steps taken should be reproducible and easy to understand. Include any custom code or references to public tools.

2.4 Vulnerability Discovery

Provide relevant analysis steps to locate vulnerability inside the application or environment, this includes results from static analysis and/or dynamic analysis. Explain the vulnerability identified.

Only the steps that ended up working are required.

2.5 Exploit or Bypass Creation

Provide a description of steps to create the exploit or security control bypass. At the end of this section the full exploit (or bypass) code should be developed while an explanation of each step should be performed.

2.6 Screenshots

The exam control panel contains a section available to submit your proof files. The contents of the local.txt, proof.txt or secret.txt files obtained from your exam machines must be submitted in the control panel before your exam has ended. Note that the control panel will not indicate whether the submitted proof is correct or not.

Each local.txt, proof.txt or secret.txt found must be shown in a screenshot that includes the contents of the file, as well as the IP address of the target by using ipconfig.